数理解析研究所講究録
549巻 1985年 1-17

整数表現に関する問題

北大理学部　吉田知行 (Tomoyuki Yoshida)

整数表現に関係した問題として，組合せ論への応用と有限群のグロタンディック環に関する話題を述べた．

§1. 有限射影平面.

最近ドイツのOttが位数10の射影平面は存在しないということを証明したと報告してこの方面の研究者に大きな衝撃を与えた．位数10というのはきわめて特殊な場合であるが，これが解ければ一般の基本予想も解けるだろうと言われるなど重要な場合である．またJ.G. Thompsonでさえ解けなかったほどの難問である．さらに，位数10の射影平面は点の個数が111個しかなく，このような射影平面の非存在は原理的には(つまり超高速の計算機があれば)解けるはずの問題である．Ottの証明は残念ながら間違っていたというが，彼のこれまでの研究発表から見て証明の方針は見当がつく．

<u>定義</u>．P を有限集合，$\mathcal{L}$ をその部分集合族とする．(P の元を点，$\mathcal{L}$ の元を直線という．) 次が成立する時，$(P, \mathcal{L})$ を<u>有限射影平面</u>という．

(P.1) 相異なる2点を通る直線はただ1本だけ存在する．

(P.2) 相異なる2直線の交点はただ1点だけ．

(P.3) 退化しない4角形が存在する．

$(P, \mathcal{L})$ が有限射影平面なら，ある自然数 $n > 1$ があって，

(i) 各直線は $n+1$ 個の点からなる．

(ii) 各点は丁度 $n+1$ 本の直線に含まれる．

(iii) $|P| = |\mathcal{L}| = n^2 + n + 1$．($=: v$ とおく．)

この n を $(P, \mathcal{L})$ の<u>位数</u>という．

<u>例</u>．普通の射影平面 $PG(2, q) = \mathbb{F}_q^{\,3} - \{0\} / \sim$ は上の公理をみたす．位数は q に等しい．

<u>基本予想</u>．有限射影平面の位数は素数巾である．

$A = (a_{p\ell})_{p \in P, \ell \in \mathcal{L}}$ を $(P, \mathcal{L})$ の結合行列とする；

$$a_{p\ell} = \begin{cases} 1 & p \in \ell \\ 0 & p \notin \ell . \end{cases}$$

Jを，どの成分も1の$v\times v$行列とする．またIは単位行列とする．このとき，次が容易に得られる．

$$(*) \qquad A\,{}^tA = nI + J.$$

逆にこの行列方程式が(0 1)行列Aを解に持てば，Aはある射影平面の結合行列である．

$x=(x_1,\cdots,x_v)$，$y:=xA=(y_1,\cdots,y_v)$をとれば，(*)より，

$$\sum y_i^2 = n\sum x_i^2 + \left(\sum x_i\right)^2$$

だから，(*)を2次形式の問題ととらえることもできる．

<u>定理</u>（BRC, Bruck-Ryser-Chowla, 1950）

位数nの射影平面が存在したと仮定し，$v=n^2+n+1$とおく．このとき，

$$(**) \qquad nx^2 + (-1)^{(v-1)/2}y^2 = z^2$$

は$(0,0,0)$でない有理整数解をもつ．

整数論によって，これは次のようにも書ける；

$n=p_1\cdots p_t n'^2$（$p_1,\cdots,p_t$は相異なる素数），$n\equiv 1,2 \pmod 4$なら，$p_i=2$または$p_i\equiv 1 \pmod 4$ $(\forall i)$．

$n\equiv 0,3 \pmod 4$のとき，$v\equiv 1 \pmod 4$となり，BRC方程式(**)は$(0,1,1)$を解にもつ．逆に次のこともわかって

いる（ホールの本の §10.3）.

行列方程式 (*) が $M_v(\mathbb{Q})$ に解をもつ

$\Leftrightarrow$ BRC 方程式 (**) が自明でない解をもつ.

例. $n=6$ となる有限射影平面は存在しない. しかし, $n=10, 12, 15, 18, 20, 24, 26, 28, \cdots$ は BRC によっても消えない. これらのパラメータを消す方法は現在のところまったく考えられない.

定義. (P, L) : 位数 n の射影平面, $v := n^2+n+1 = |P|$.

$I := \{(p, \ell) \in P \times L \mid p \in \ell\} \subseteq P \times L$.

$V := \mathbb{Z}[I]$: I を基底とする自由アーベル群.

$\sigma, \tau \in \mathrm{End}_{\mathbb{Z}}(V)$ を次で定義する.

$$\sigma : (p, \ell) \longmapsto \sum_{q \in \ell;\, q \neq p} (q, \ell)$$

$$\tau : (p, \ell) \longmapsto \sum_{m \in L :\, p \in m \neq \ell} (p, m)$$

σ と τ で生成された $\mathrm{End}_{\mathbb{Z}}(V)$ の部分環 H を (P, L) の Hecke 環という.

H はアーベル群としては基底 $\{1, \sigma, \tau, \sigma\tau, \tau\sigma, \sigma\tau\sigma\}$ を持つ自由アーベル群であり, 次の基本関係式をもつ:

$$\begin{cases} \sigma^2 = n + (n-1)\sigma \\ \tau^2 = n + (n-1)\tau \\ \tau\sigma\tau = \sigma\tau\sigma \end{cases}$$

例. $n = q$ = 素数巾のとき, H は A_2 型 Weyl 群の Hecke 環に同型である. つまり, $G = GL_3(q)$, B = Borel = {下3角行列} としたとき,

$$H \cong \mathbb{Z}[B\backslash G/B] \cong \mathrm{End}_{\mathbb{Z}G}(\mathbb{Z}[G/B]).$$

以下 Hecke 環 H とその上の標準加群 V の性質をかかげておく.

① V は忠実な H-加群.

② V 上の内積が, $\langle (p,\ell),(q,m)\rangle := \delta_{pq}\,\delta_{\ell m}$ で定義され, σ と τ はこの内積に関して自己随伴: $\langle x, \sigma y\rangle = \langle \sigma x, y\rangle$ 等.

③ $\sigma \mapsto \sigma$, $\tau \mapsto \tau$ は H の逆自己同型を与える.

④ $H_{\mathbb{Q}} := \mathbb{Q}\otimes_{\mathbb{Z}} H$ は半単純で, $\mathbb{Q}\oplus\mathbb{Q}\oplus M_2(\mathbb{Q})$ に同型. $H_{\mathbb{Q}}$ は3個の既約表現をもつ:

ind : $\sigma \mapsto n$, $\tau \mapsto n$

st : $\sigma \mapsto -1$, $\tau \mapsto -1$ (Steinberg表現)

f : $\sigma \mapsto \begin{pmatrix} -1 & 1 \\ 0 & n \end{pmatrix}$, $\tau \mapsto \begin{pmatrix} n & 0 \\ n & -1 \end{pmatrix}$

⑤ $V_{\mathbb{Q}} := \mathbb{Q} \otimes_{\mathbb{Z}} V$. このとき、上の既約表現に対応した部分空間 $V_{\mathbb{Q}}^{ind}$, $V_{\mathbb{Q}}^{st}$, $V_{\mathbb{Q}}^{f}$ をとると、

$$V_{\mathbb{Q}}^{ind} = \mathbb{Q}\, \iota \qquad \iota := \sum_{(p,\ell)\in I} (p,\ell) \in V$$

$$\dim V_{\mathbb{Q}}^{st} = n^3 \qquad V_{\mathbb{Q}} = V_{\mathbb{Q}}^{ind} \perp V_{\mathbb{Q}}^{st} \perp V_{\mathbb{Q}}^{f}.$$

$$\dim V_{\mathbb{Q}}^{f} = 2n^2 + 2n.$$

Ott はこのような $H_{\mathbb{Q}}$, $V_{\mathbb{Q}}$ の研究によってBRCの定理の興味ある証明を得た. つまり $H_{\mathbb{Q}}$ の作用の方から $V_{\mathbb{Q}}$ に入る非退化対称2次形式の判別式 α を求め、一方基底 I から計算される判別式は1なので、$\alpha \in \mathbb{Q}^{*2}$ を得る. これからBRCが従がう. 彼の方針は $\mathbb{Q}$ でなくとも適用できると思われる.

R を剰余標数 p の離散付値環(商体は標数0), $F := R/J(R)$ (標数 p の体)とする. Ott による基本予想解決のプログラム(?)は概略次のようなものとなる.

(1) H_R $(:= R\otimes H)$ や H_F の(直)既約表現を求める.

(2) V_R $(:= R\otimes V)$ や V_F の(直交)直和分解(またはWitt群のような適当なグロタンディンク群での分解)

(3) V_R, V_F の不変量(2次形式の判別式など)の計算.

この方針でうまく行く保障はまったくないが、標数 p としては n を割る素数をとるのがよさそうである, その場合 H_R

はGorenstein order（即ち，H_R 自身が，H_R-lattice のカテゴリーで入射的）だし，$p \| n$ のときはさらに遺伝的（すべての左イデアルが射影的）で直既約 H_R-lattice は4個しかないことがわかる．（$p | n$ のときの H_R は有限表現型かもしれない）．

次に注意すべきなのは2次形式 $\langle\ ,\ \rangle : V_R \times V_R \to R$ を H_R 上の非退化エルミート形式 $[\ ,\ ] : V_R \times V_R \to H_K$ に拡張しておくのがよい．

（KはRの商の体）

$(p,l),(q,m) \in I$ に対し，$[(p,l),(q,m)] \in H_K$ を

1	if	$p=q,\ l=m$
σ/n	if	$p\neq q,\ l=m$
τ/n	if	$p=q,\ l\neq m$
$\sigma\tau/n^2$	if	$p\in l-m,\ q\in l\cap m,$
$\tau\sigma/n^2$	if	$p\in l\cap m,\ q\in m-l$
$\sigma\tau\sigma/n^3$	if	$p\in l-m,\ q\in m-l$

で定義する．このとき，$u,v\in V_R$ に対し，

$$[hu, h'v] = h[u,v]\overline{h'} \qquad h,h'\in H_R$$

ここで，$h \longmapsto \bar{h}$ は σ と τ を動かさない H_R の逆自己同型．

こうすると問題は H_R 上のエルミート形式の分類というポピュラーなものになる．

以上述べたと同様のことは，もっと一般の対称デザインにも考えられる．また強正則グラフ，距離正則グラフ（もっと一般の association scheme）については Hecke 環が可換なので射影平面の場合より話は簡単になる．だが簡単と言っても最後に帰着される Hecke 環上の加群と2次形式の問題は整数論がからんで来て解きにくいことも多い．最も簡単な強正則グラフの場合，問題は実2次体（とそこの整数環）上のエルミート加群の分類になるが，これもむずかしい（Ott の論文の §2）

§2．いろいろな Hecke 環の作用．

G を有限群，H をその部分群とする．このとき，

$$(HxH)\cdot(HyH) := \sum_{z\in H\backslash G/H} |(HxH \cap zHy^{-1}H)/H| \cdot (HzH)$$

（ここで z は $H\backslash G/H$ の完全代表系上を動く）とすることによって，$\mathbb{Z}[H\backslash G/H]$ は Hecke 環と呼ばれる環になる．この環は自己準同型環 $End_{\mathbb{Z}G}(\mathbb{Z}[G/H])$ に同型である；

$$(HxH):\ gH \longmapsto \sum_{uH\in HxH/H} guH$$

次に $\mathcal{H}_{\mathbb{Z}G}$ を permutation $\mathbb{Z}G$ 加群のなすカテゴリーとする．これは $\mathbb{Z}G$ 加群のカテゴリ $\mathcal{M}_{\mathbb{Z}G}$ の full subcategory で，abelian ではないが additive である．

もし $\mathcal{H}_{\mathbb{Z}G}$ からアーベル群のカテゴリーへの関手 F があれ

ば，各 $H \leq G$ に対し，$F(\mathbb{Z}[G/H])$ は自然に（右）$\mathbb{Z}[H\backslash G/H]$ 加群となる．良く知られた例は，G 加群 V に対し，

$$V^H := \{ v \in V \mid vh = v \quad \forall h \in H \}$$

が $\mathbb{Z}[H\backslash G/H]$ 加群になることである．この作用は関手 $\mathbb{Z}X \longmapsto \mathrm{Map}_G(X, V)$ から従がう．Hecke環の作用をこのようにとらえた論文がいくつか出ている．

S/R を可換環の有限次ガロア拡大，そのガロア群を G とする．$R = S^G$ である．（そのような拡大の例としては，代数体の有限次ガロア拡大 L/K に対し，R と S をそれぞれ K，L の整数環とすれば，L/K が不分岐のとき，S/R がガロア拡大となる）．このとき，

__定理__．（Roggenkamp・Scott，Fordなど）$\forall H \leq G$ に対し，$U(S^H)$，$\mathrm{Pic}(S^H)$，$\mathrm{Br}(S^H)$，$C(L^H)$ は $\mathbb{Z}[H\backslash G/H]$ 加群である．これらは関手 $\mathcal{H}_{\mathbb{Z}G} \longrightarrow \underline{\mathcal{A}b}$; $\mathbb{Z}[H\backslash G] \longmapsto U(S^H)$，$\mathrm{Pic}(S^H)$，$\mathrm{Br}(S^H)$，$C(L^H)$ から得られる．（$C(L^H)$ は代数体の場合の類群）．

この定理の証明において本質的なのは，トレースとかノルムとかtransferとか呼ばれる写像が存在していわゆるMackey分解をみたすことである．

さて，このようなHecke環の作用と，有限群の置換表現の理論を組み合わせてみよう．

L/K を代数体のガロア群，G をガロア群，$p \neq q$ を素数，H を G の (q,q) 型の部分群，$H_0, \cdots, H_q$ を H の位数 q の部分群とする．$\hat{\mathbb{Z}}_p$ を p 進整数環とする．このとき，次の同型がある．

$$\hat{\mathbb{Z}}_p G \oplus (\hat{\mathbb{Z}}_p[G/H])^{(q)} \cong \bigoplus_{i=0}^{q} \mathbb{Z}_p[G/H_i].$$

この同型に上の関手を作用させると，例えば，

$$C(K)_p \oplus (C(K^H))_p^{(q)} \cong \bigoplus_{i=0}^{q} (C(K^{H_i}))_p$$

を得る．ここで $C(K)_p$ は類群の Sylow p 群．位数をとると良く知られた類数の関係が得られる．

同様にゼータ関数の間の等式がある：

$$\zeta_K(s)\, \zeta_{L^H}(s)^q = \prod_{i=0}^{q} \zeta_{L^{H_i}}(s)$$

Wielandt の位数公式も同じ形をしているが，これも同じ方法で証明される：$A \leq Aut(G)$，$(|A|,|G|)=1$，$A \cong (\mathbb{Z}/q\mathbb{Z})^2$，$q$ は素数のとき，

$$|C_G(A)| = |G|^{-q} \prod_{1 \neq B \lneq A} |C_G(B)|.$$

§3．置換加群の同型と induction 定理．

一般には，有限 G 集合 X，Y が $\mathbb{Z}X \cong \mathbb{Z}Y$ ($\mathbb{Z}G$ 加群と

して）であっても，$X \cong Y$とは言えない．有限G集合のカテゴリーの直和と直積に関するGrothendieck環をBurnside環といい，$\Omega(G)$で表わす．有限生成$\mathbb{Z}G$加群のカテゴリーの直和とテンソル積に関するGrothendieck環を表現環と言い$a(G)$で表わす．自然な環準同型 $f: \Omega(G) \longrightarrow a(\mathbb{Z}G)$ $: [X] \longmapsto [\mathbb{Z}X]$がある．

<u>定理</u>（Dress） $f: \Omega(G) \longrightarrow a(G)$が単射

$\Leftrightarrow$ (*) ある素数pと正規p-部分群Pに対して，

G/Pが巡回群．

したがってGが(*)をみたさないなら，ある有限G集合XとYが存在して，$X \not\cong Y$だが$\mathbb{Z}X \cong \mathbb{Z}Y$となる．この事実に前節の考えを応用してみよう．

L/Kを代数体の有限次ガロア拡大，Gをそのガロア群とする．XとYを有限G集合で$\mathbb{Z}X \cong \mathbb{Z}Y$なるものとする．このとき$Map_G(X, L)$は中間体の直和である（実際，$X \cong G/H_1 + \cdots \Rightarrow Map_G(X, L) \cong L^{H_1} \times \cdots$）．しかも$\mathbb{Z}X \cong \mathbb{Z}Y$より，$Map_G(X, L) \cong Map_G(Y, L)$（$K$多元環として）が得られる．とくに類群をとると，

$$C(Map_G(X, L)) \cong C(Map_G(Y, L)).$$

同様の同型が，ブラウアー群Br，ピカール群Pic，単数群Uさらに高次のコホモロジー群についても得られる．

さて，(＊) をみたさない群 G が与えられたとき，$X \not\cong Y$ だが $\mathbb{Z}X \cong \mathbb{Z}Y$ となる有限 G 集合 X, Y を求めたい．そのためには Burnside 環のベキ等元公式が使える．

<u>定理</u>．G を有限群，μ を G の部分群束の Möbius 関数とする．

(i) $\mathbb{Q} \otimes_{\mathbb{Z}} \Omega(G)$ の原始ベキ等元は，

$$e_{G,H} := \frac{1}{|N_G(H)|} \sum_{D \leq H} |D| \mu(D, H) [G/D]$$

の形をしている．ここで $H \leq G$ で，H と H' が共役 $\Leftrightarrow$ $e_{G,H} = e_{G,H'}$．したがって，$\mathbb{Q} \otimes \Omega(G)$ の原始ベキ等元 $\longleftrightarrow$ G の部分群の共役類．

(ii) p を素数，$\mathbb{Z}_{(p)} := \{a/b \in \mathbb{Q} \mid a \in \mathbb{Z}, b \in \mathbb{Z} - p\mathbb{Z}\} \leq \mathbb{Q}$ とおく．このとき，$\mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} \Omega(G)$ の原始ベキ等元は，

$$e^p_{G,H} = \sum_{(K):\, O^p(K) \sim H} e_{G,K}$$

の形をしている．ここで，$O^p(K) = \langle p'\text{-element of } K \rangle$，で，$(K)$ は G の部分群の共役類で $O^p(K)$ と H が共役なものを動く．

この公式は Gluck，吉田によって得られた．次が目標の定理である．

<u>定理</u>．Gを有限群，Hをその部分群群とする．

(i) どの素数pに対しても$H/O_p(H)$は巡回群でないとする．ここで$O_p(H)$は最大の正規p部分群．

$$|G|\cdot e_{G,H} = [X] - [Y]$$

をみたすG集合X，Yをとる．このとき$\mathbb{Z}X \cong \mathbb{Z}Y$．

(ii) pを素数とし，$H/O_p(H)$は巡回群でなく，$O^p(H)=H$（即ちHは指数pの正規部分群をもたない）とする．

$$|G|\cdot e^p_{G,H} = [X] - [Y]$$

をみたすG集合X，Yをとる．このとき$\mathbb{Z}_{(p)}X \cong \mathbb{Z}_{(p)}Y$．

証明の概略．Dress による induction 定理（後述）によれば，

$$|G|\cdot 1_G = \sum_i a_i[\mathrm{Ind}^G_{H_i}(M_i)], \quad in\ a(\mathbb{Z}G)$$

ここで$a_i \in \mathbb{Z}$，$H_i \leq G$，$H_i/O_{p_i}(H_i)$は巡回群（p_iは素数），M_iは$\mathbb{Z}H_i$加群，となる．Frobenius の相互律より

$$f(e_{G,H})\ [\mathrm{Ind}^G_{H_i}(M_i)]$$
$$= \mathrm{Ind}^G_{H_i}(f(\mathrm{Res}^G_{H_i}(e_{G,H}))\cdot[M_i]$$

しかしHの共役はH_iに入らないので，$\mathrm{Res}^G_{H_i}(e_{G,H})=0$．よって，$f(e_{G,H})[\mathrm{Ind}^G_{H_i}(M_i)]=0$　$\therefore |G|\ f(e_{G,H})=0$．

これは$[\mathbb{Z}X]=[\mathbb{Z}Y]$，即ち$\mathbb{Z}X \cong \mathbb{Z}Y$を意味する．

(ii)も同様に証明される．

§4. 文献紹介.

有限群とorderの整数表現の概説はReinerによる[1]と[2]がくわしい. [2]はintroductionに11個の問題があり, この方面で重要な問題点がわかるのがありがたい. また[2]はやさしく書かれていて読みやすい. 文献のリストは[1]と[3]に多数のっている. [3]は歴史的文献も含んでいる. [3]は各分野(2次形式, 代数的整数論, 虚数乗法論, トポロジー, 結晶理論)において整数表現がどのように現われているかを紹介している. 整数表現全般について, [4]～[7]も役に立つ. [5]は新しい情報も含んでいる. この続巻もまもなく出版されるという.

K理論との関係では[8], [9], [10]がある.

有限幾何については[11], [12].

いろいろなHecke actionについては[13]～[16].

Burnside環については[19], [20], [21]. 中等元公式のinduction定理への応用については[20]. [22]は読みにくいがきわめて含蓄に富んでいる.

相対Grothendieck環については[23], [24]. LamとReinerの一連の論文はこの方面の問題点を明らかにしている.

References

1. I. Reiner, A survey of integral representation theory, Bull. A. M. S. 76 (1970), 159-227.

2. I. Reiner, Topics in integral representation theory, Springer Lecture Notes 744 (1979), 1-143.

3. W. H. Gustafson, Remarks on the history and applications of integral representations, Springer Lecture Notes 882 (1980), 1-36.

4. C.W.Curtis-I.Reiner, Representation theory of finite groups and associative algebras, Interscience, New York, 1962.

5. C.W.Curtis-I.Reiner, Methods of representation theory I, Interscience, New York, 1981.

6. I.Reiner, Maximal order, Academic Press, London, 1975.

7. K.Roggenkamp, Lattices over orders I,II, Springer Lecture Notes 115 (1970) and 142 (1970).

8. H.Bass, Algebraic K-theory, Benjamin, New York, 1968.

9. Milnor, Introduction to algebraic K-theory, Princeton, 1971.

10. R.Swan-E.Evans, K-theory of finite groups and orders, Springer Lecture Notes 149 (1970).

11. U.Ott, Some remarks on representation theory in finite geometry, Springer Lecture Notes, 893 (1981).

12. M.Hall, Combinatorial theory, Blaisdell, 1967.

13. T. Yoshida, On G-functor II : Hecke oprators and G-functors, J. Math. Soc. Japan, 35 (1983), 179-190.

14. D. Husemoller, Burnside ring of a Galois group and the relations between zeta functions of intermediate fields, Proc. Symp. in Pure Math., 37 (1980), 603-610.

15. K. Roggenkamp-L. Scott, Hecke action on Picard groups, J. Pyre Appl. Algebra 26 (1982), 85-100.

16. T.J.Ford, Hecke actions on Brauer groups, j. Pure Appl. Algebra 33 (1984), 11-17.

17. C. Walter, Brauer's class number relatin, Acta Arith. 35 (1979), 33-40.

18. R. Perlis, On the class numbers of arithmetically equivalent fields, J.Number theory 10 (1078), 488-509.

19. D. Gluck, Idempotent formula for the Burnside algebra with applications to the p-subgroup simplicial complex, Illinois J. Math. 25 (1981), 63-67.

20. T. Yoshida, Idempotents of Burnside rings and Dress induction theorem, J. Algebra 80 (1983), 90-105.

21. T. tom Dieck, Transformation groups and representation theory, Lectur Notes in Math. 766, Springer, Berlin, 1979.

22. A. Dress, Contributions to the theory of induced representations, Springer Lecture Notes 342 (1973),183-240.

23. A.Dress, On relative Grothendieck rings, Springer Lecture Notes 488 (1974), 79-131.

24. T.Y.Lam-I.Reiner, Restriction maps on relative Grothendieck rings, J.Algebra, 14 (1970), 260-298.